PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-091427

(43)Date of publication of application : 10.04.1998

(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 09-151747

(22)Date of filing : 10.06.1997

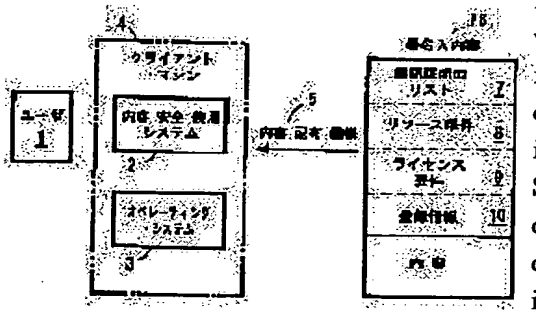
(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>

(72)Inventor : ANAND RANGACHARI
ISLAM NAYEEM
RAO JOSYULA RAMACHANDRA

(30)Priority

Priority number : 96 661687 Priority date : 11.06.1996 Priority country : US

(54) METHOD AND SYSTEM FOR GUARANTEEING SAFETY IN USING CONTENTS WITH SIGNATURE



(57)Abstract:

PROBLEM TO BE SOLVED: To safely execute a software from an unreliable source by providing an analyzing module which is an extracting device extracting a signature part from contents with a signature and executing correction when a doubt exists in reliability and safety and a reinforcing module which guarantees that a usage of contents with a signature coincides with a resource important matter and an admission certification.

SOLUTION: A user 1 uses a client machine 4 and uses content distributing mechanism 5 for transferring the contents 6 with the signature to its machine. The contents is provided with the signature, the signature has four blands and the first blank 7 is the list of a software admission certification. The contents with the signature is down-loaded by a content importing system. The extracting device analyzes the blanks of the signature and gives the information to the analyzing module. The analyzing module recognizes safety, investigates the list of the admission certification in security and decides a reliability level. The analyzing module investigates and decides the resource important matter so as to give the information to the reinforcing module.

CLAIMS

[Claim(s)]

[Claim 1] It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, When [which the above-mentioned extractor supplied] the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are The contents insurance use system used in the computer system characterized by having the analysis module which takes amendment actuation, and the strengthening module which guarantees that use of contents with a signature is in agreement with the requirements for a resource, and approval certification.

[Claim 2] The above-mentioned extractor is a system according to claim 1 characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

[Claim 3] It is the system according to claim 1 which the above-mentioned extractor has further a means to extract license conditions from a signature, and is characterized by guaranteeing that the above-mentioned strengthening module's performing an operating system and a dialogue and using these contents corresponds with license conditions.

[Claim 4] It is the system according to claim 1 carry out having further the DS stored in the memory of the above-mentioned computer system, and the above-mentioned DS having the table showing correspondence between a user, approval certification, and the function of contents with a signature, and having a means strengthen this use when the above-mentioned strengthening module is connected so that a correspondence table may be read from DS, and a user uses contents with a signature according to the above-mentioned correspondence as the description.

[Claim 5] The above-mentioned strengthening module is a system according to claim 1 characterized by having a means to guarantee that pursue the process generated from contents with a signature, and actuation of this process is in agreement with the requirements for a resource, and approval certification.

[Claim 6] The above-mentioned import device is a system according to claim 1 characterized by being the communication channel connected to the communication network.

[Claim 7] The above-mentioned import device is a system according to claim 1 characterized by being rotation storage.

[Claim 8] The above-mentioned import device is a system according to claim 1 characterized by being the memory card in which desorption is possible.

[Claim 9] It is the system according to claim 1 which has further the DS stored in the memory of the

above-mentioned computer system, and is characterized by the above-mentioned DS having the table showing correspondence between the limits of one of the resources which the actual resource and the above-mentioned computer system which contents with a signature, the requirements for a resource, and contents with a signature consumed imposed on contents with a signature.

[Claim 10] The above-mentioned table is a system according to claim 9 characterized by license conditions including further the constraint on the use imposed on contents with a signature.

[Claim 11] It is the memory which can read the computer which installed contents with a signature. The above-mentioned contents with a signature include the contents which can read the signature which can read a computer, and a computer. The signature which can read the above-mentioned computer in order to use the contents which can read the approval certification column and computer which are contained in the distribution chain of the contents which can read the above-mentioned computer, and which include code discernment of sending agency equipment and repeating installation at least It has two or more columns containing the requirements column for a resource which identifies a required computing resource.

[Claim 12] It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the license conditions [the above-mentioned part] which can read the computer relevant to the above-mentioned contents, The contents use system used in the computer system characterized by having the strengthening module which controls actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.

[Claim 13] The above-mentioned extractor is a system according to claim 1 characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

[Claim 14] They are the step which imports contents with a signature into computer system, and the step which extracts the part of a signature from contents with a signature. The above-mentioned step including the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, The step which takes amendment actuation when the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are, The step which controls the operating system of the above-mentioned computer system to guarantee that use of contents with a signature does not exceed the requirements for a resource, and approval certification, How to guarantee the insurance of use of the contents with a signature in the above-mentioned computer system characterized by ****(ing).

[Claim 15] The approach according to claim 14 characterized by having further the step registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.

[Claim 16] The approach according to claim 14 characterized by having further the step which controls the above-mentioned operating system to guarantee that extract license conditions from a signature and contents with a signature are in agreement with license conditions.

[Claim 17] The approach according to claim 14 characterized by having further the step which forms the DS containing the table showing correspondence between the certification of a user and approval, and the function of contents with a signature in the memory of the above-mentioned computer system, and the step which strengthens this use when a user uses contents with a signature according to the above-mentioned correspondence.

[Claim 18] The approach according to claim 14 characterized by having further the step which operates the above-mentioned process compulsorily so that it may be in agreement with the step and the requirements for a resource which pursue the process generated from contents with a signature, and approval certification.

[Claim 19] The contents with a signature are approaches according to claim 14 characterized by having at least one of an application program and documents.

[Claim 20] How to control use of the contents in the above-mentioned computer system characterized by to have the step which imports into computer system contents including the license conditions which can read a computer, the step which extract the license conditions which can read a computer from the contents which imported, and the step which control actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.

[Claim 21] The approach according to claim 20 characterized by having further the step automatically registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the security device of the computer for performing safely software which came to hand with the means of a network or others from the unreliable source.

[0002]

[Description of the Prior Art] Since the usefulness of the computer connected by network is increased, it searches for the approach of making it possible to execute the program which these computers received from the server. The main advantages of such a system at the time of seeing from a user are that the amount of the software which must be stored in a user's computer decreases by this. Although this system has many advantages when it sees from the developer of

software, main advantages are that the provider of application can control more to distribution of a program. Use of the Java applet (namely, program) embedded on the document of World Wide Web is an example which such a system is large and has spread.

[0003] The software acquired from the server means improper use, and the important concerns to such approach damage a user's computer, or will steal [hear / I / **********] data, and there are. Therefore, the downloaded software must give only the resource of the system which these need, and the thing beyond it must be performed by the controlled environment which is not given. The main troubles of the security device of the Java applet used now are that this does not have sufficient flexibility. Java applets are considered [no] to be hostile things, and accessing the resource of most on the operating system of a user's machine is allowed.

[0004] Various things exist in the standard technique for authentication by the public key cryptosystem. RSA is an example of the public-key-encryption algorithm currently used broadly. RSAref and PGP are contained in the example of activation of this.

[0005] The device which creates a digital signature to a message exists again. These signatures connect the contents of the message to people. These can be used again, in order to create a digital signature to a message so that the implementer of a message cannot avoid responsibility for this message. The MD5 algorithm combined with RSA is an example of a signature system.

[0006] The capacity for controlling access to the resource of a system is being used for many computer operating systems. One capacity is authorization holding a process, in order to perform a certain action to other objects. There are Amoeba and Mach in the prominent operating system which is using the capacity for strengthening security.

[0007]

[Problem(s) to be Solved by the Invention] Therefore, the purpose of this invention is offering the security device for performing safely software which came to hand on a network or other means from the unreliable source.

[0008]

[Means for Solving the Problem] According to the 1st aspect of affairs of this invention, the contents insurance use system and approach of using it in computer system are offered. This system is connected so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor with which it is the extractor which extracts the part of a signature from the above-mentioned contents with a signature, and the above-mentioned part includes the approval certification relevant to the above-mentioned contents, The requirements for a resource which use the above-mentioned contents, and the analysis module which takes amendment actuation when [which the above-mentioned extractor supplied] the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are, It has the strengthening module which guarantees that use of contents with a signature is in agreement with the requirements for a resource, and approval certification.

[0009] According to the 2nd aspect of affairs of this invention, the memory which can read the

computer which installed contents with a signature is offered. These contents with a signature have two or more columns containing the requirements column for a resource which identifies an operation resource required in order that the signature which can read a computer may use the contents which can read the approval certification column and the computer which are contained in the distribution chain of the contents which can read a computer, and which include code discernment of sending agency equipment and repeating installation at least including the contents which can read the signature which can read a computer, and a computer.

[0010] According to the 2nd aspect of affairs of this invention, the contents use system and approach of strengthening license conditions within computer system are offered. This system is connected so that the contents with a signature which imported according to a contents import device and the above-mentioned import device receive, it is the extractor which extracts the part of a signature from the above-mentioned contents with a signature, and an above-mentioned part has an above-mentioned extractor including the license conditions which can read the computer relevant to the above-mentioned contents, and the strengthening module control actuation of the above-mentioned computer system to guarantee that it is in agreement to license conditions in use of contents with a signature.

[0011]

[Embodiment of the Invention] The example of this invention is explained to a detail with reference to drawing. Drawing 1 summarizes and explains this invention. A user 1 uses the contents distribution device 5 for using a client machine 4 and transmitting the contents 6 with a signature to the machine. A floppy disk, CD-ROM, and the Internet are contained in the example of this distribution device. A Java applet, OLE KOMPONENTSU, and SOM KOMPONENTSU are contained in the example of the contents which can be performed. These contents have the signature. The contents of other classes can include a text, voice, and an image. A signature has four columns and the 1st column 7 is a list of approval certification of software. Drawing 3 explains this to a detail further. Discernment of the author and a manufacturer is included in the example of approval certification. These certification guarantees that the certification is created and distributed by him who is indicated by the list. Furthermore, these certification offers a means to confirm that modification is not added to these contents, after signing the contents. Furthermore, these certification offers further a means to guarantee that the author cannot avoid responsibility for the created contents. The 2nd column 8 has described the computing resource 3 which the contents need on the machine of a client. These resources are needed in order that these contents may attain that purpose on a client machine. Install and activation of contents with a signature are included in the example of this purpose. Access, RAM and CPU, and the capacity and the user display of a network to the tooth space of a disk, the tooth space of a file, and a file are included in the example of a computing resource.

[0012] If contents with a signature are downloaded in a user's machine, a user can use these contents by various approaches. Performing installing this, viewing this, and this is included in the example which uses these contents. These contents are used in the environment carefully controlled

on the machine of a client. In order to use contents with a signature in this way, it is necessary to access an operation resource on the machine of a client. A resource required in order to use the contents 8 with a signature is a part of signature of the contents. Access to such a resource is arbitrated by the contents insurance use system 2.

[0013] The 3rd column (this is an option) offers the license information 9. A service condition like the number of the machines which can use the contents, and a period is included in the example of license information. The 4th column (this is an option) is the registration information 10. This information is used in order to register the contents into a provider automatically. Drawing 2 shows an example of a contents distribution device. These contents occur on the machines 15 and 16 of a manufacturer or the author, and 17, and before downloading in the machine 11 of a client, they go via many middle machines 12, 13, and 14.

[0014] Drawing 3 shows the certification accumulated in these contents with a signature according to contents with a signature being distributed to a user's machine 20 from a manufacturer's machine 22. A manufacturer attaches approval certification to these contents, before transmitting the contents 25 with a signature to repeating installation 21 with a certain means 27. Next, this repeating installation attaches that approval certification to these contents with a signature, before transmitting the contents 24 with a signature to the next repeating installation in a distribution chain. If contents with a signature finally reach a user by such approach, this includes the list of approval certification of all repeating installation and manufacturers 23.

[0015] Drawing 4 shows the process which downloads contents with a signature from the provider 31 of the contents within the contents insurance use system 31, and the process following this. This contents insurance use system 31 is IBM. PC personal computer, IBM It can carry out as a part of general purpose computer system (not shown) like which workstation of the others suitable for using it as a RS/6000 workstation or a system of a client. These contents with a signature are downloaded by the contents import system 33. An extractor 34 analyzes the column of a signature and hands over this information to the analysis module 35. This analysis module checks the integrity of the contents. Next, this analysis module considers the list of approval certification of security, and judges access in the case of using these contents by that machine, and the level of dependability. Next, if this analysis module examines the requirements for a resource of these contents and can do them, it will judge whether these requirements can be satisfied by a user's input. Next, this information is handed over to contents interpretation equipment 36 and the strengthening module 37.

[0016] The contents import device 33 is a network interface (for example, a user is connectable with the Internet with this), a diskette subsystem, and CD. It can carry out as a ROM subsystem or a cartridge storage subsystem. An extractor 34, the analysis module 35, and contents interpretation equipment 36 and the strengthening module 37 can be carried out as a program code which can be performed by workstation which performs safe contents. As for a strengthening module, it is desirable to connect with the operating system (for it to be (like OS/2, UNIX, or Windows NT)) of a workstation. Contents interpretation equipment 36 can be carried out as a module in an operating

system, or can be made separate from an operating system like a Java interpreter program.

[0017] Drawing 9 is a flow chart corresponding to actuation of the system of drawing 4 . Contents interpretation equipment is a device which uses the contents. The Internet browser and a Java virtual machine are contained in the example of contents interpretation equipment. A strengthening module uses the level of the dependability which the analysis module judged, and creates an item in an access information table. Drawing 5 explains this table.

[0018] In order to use contents with a signature, generally it is necessary to access the resource of an operating system. Drawing 5 shows the table 40 which a strengthening module uses, in order to pursue the resource which is the contents with a signature currently used on that machine and which these contents consumed, or it required. A strengthening module uses the approval certification 41 about the contents with a signature, and judges the limit of a resource 42 where these contents with a signature should be given on the machine of a client. This judgment can be performed by various approaches including the demand of a clear input to the user for judging access which the prior configuration and the prior contents on a table should obtain. It is efficient that a strengthening module creates the capacity reflecting "who accesses what [how many]" for contents with a signature. Generally, the resource which contents with a signature obtain is the subset of the resource which a user accesses on the machine of a client. A security manager pursues the resource 43 consumed according to the contents. This is attained by guaranteeing that all accesses to the resource of the system by contents with a signature pass a security manager. This table includes the item over the resource 43 which contents with a signature required again. If the consumed resource 43 exceeds the limit 42 of a resource, or the demanded resource 44 at which time, a security manager can take amendment action. The inquiry to termination of use of contents with a signature and the user of the guidance about how it goes on is included in the example of amendment action.

[0019] Drawing 6 shows the relation between the capacity of various items. A user's privilege 51 is the subset of the privilege of an operating system 50. The contents with a signature are performed within the environment where the privilege 52 is the subset of a user's privilege. Next, the privilege of the contents 53 with a signature is the subset of the execution environment. Other contents can be used on the machine of a client by using contents with a signature. For example, the contents in which other activation is possible are installable in the process on the machine of a client by performing a Java applet. Thus, the privilege of the generated contents 54 is the subset of the privilege which was in agreement with contents with a signature. I want to care about that the effective device for fulfilling these constraint is given to a security manager by including the requirements for a resource in the signature of contents with a signature. These generated contents can be performed as long as the resource which this consumes is the limit of the resource imposed on contents with a signature. The whole of this information can be pursued within the table of the security manager who shows drawing 5 .

[0020] If contents with a signature are downloaded in a user's machine, a user will acquire the capacity which uses these contents. This capacity is connected with the user who started the

transfer. This user allows other users to use these contents with a signature by that machine. Drawing 7 shows the relation between the privilege of other users like 61, 62, and 63, and a user's 27 privilege currently installed. For example, it will be reflected in the ability of this document to be changed [whether this user can read this document, a user's privilege can be written in this document, or] if contents with a signature are the documents of Lotus.

[0021] Drawing 8 shows the example which is Java applet 80 which contents with a signature signed. The approval certification 79 on this applet is the approval certification of that author, a manufacturer, and a retailer. This applet exists on the machine 77 of a server, and is managed according to the process 78 of a server. The machine of a server and the process of a server are mere distribution devices, and it is necessary to care about that these do not need to have any relation with the author. A contents distribution device is the Internet 76.

[0022] The agent 72 of the client which acts for a user 71 and exists on the machine 70 of a client downloads an applet by contacting the process of a server. The agent of this client sends that approval certification like discernment (that public key or certification) of a user, or discernment (IP address etc.) of the machine of a client to the process of a server. A server process uses this information, proves that a user can trust it, and pursues use of an applet. Answering this, the process of a server returns the public key (or certification) of discernment of the machine of an applet with a signature, and a server, and the process of this server to a client. A server must encipher the response with a user's public key, and it must guarantee that an applet is conveyed by the machine of a client at insurance.

[0023] The agent of a client checks the integrity of the contents, and a related signature. If this is performed, the agent of a client will judge the requirements for a resource of the certification of approval, and contents with a signature. This agent decodes the response of a server using that secrecy decode key, and extracts the security information in a response (it is (like a public key or certification)), i.e., discernment of an implementer, and discernment (it is (like a public key or certification)) of the process of a server and discernment (it is (like an IP address)) of the machine of a server. This information is supplied [user / the identifier of an applet, the requirements for a resource described in the signature, and] to security strengthening equipment 74 with discernment of the machine of a client. The approval certification of the signed applet is stored as capacity constituted by TORIPURU constituted by the identifier of contents with a signature, and the requirements for a resource described [which were described and were approval-proved], and is given to a security manager.

[0024] Security strengthening equipment is similar to the security manager in the environment of time amount where Java is operating. It is a system service with the reliance which cannot be changed. This calculates the capacity that an applet can be performed on the machine of a client using the approval certification of contents with a signature. A set of contents with a signature on activation amends all calls to the resource of a system through a security manager. This security manager uses the capacity relevant to an applet, and judges whether the resource which the applet required is permitted (drawing 10). This manager can be used in order to program the range of the

policy of security, and it can opt for access which an applet with a signature has to the resource of a system. Access is clearly permitted by promoting a user with a dialog box starting with an easy policy like access that the range of this policy has no access, and perfect, and access which the user constituted beforehand.

[0025] The user who downloads an applet judges whom [other] access to this is permitted. Special capacity is made to each user. When the contents perform this, these contents perform this by the subset of a call person's access privilege. As for a security manager, the capacity given to the user of an applet can be canceled at any times.

[0026] Although the suitable example explained this invention, this contractor can make various modification and improvements. Therefore, he has to understand that this suitable example is not what is offered as one example and means limitation. The range of this invention is clarified by the above-mentioned claim.

[0027] As a conclusion, the following matters are indicated about the configuration of this invention.

(1) It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, When [which the above-mentioned extractor supplied] the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are The contents insurance use system used in the computer system characterized by having the analysis module which takes amendment actuation, and the strengthening module which guarantees that use of contents with a signature is in agreement with the requirements for a resource, and approval certification.

(2) The above-mentioned extractor is the system of the above-mentioned (1) publication characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

(3) It is the system of the above-mentioned (1) publication which the above-mentioned extractor has further a means to extract license conditions from a signature, and is characterized by guaranteeing that the above-mentioned strengthening module's performing an operating system and a dialogue and using these contents corresponds with license conditions.

(4) the above -- computer system -- memory -- having stored -- DS -- further -- having -- the above -- DS -- a user -- approval -- certification -- and -- a signature -- entering -- the contents -- a function -- between -- correspondence -- being shown -- a table -- having -- the above -- strengthening -- a module -- DS -- from -- correspondence -- a table -- reading -- as -- connecting -- having -- the above -- correspondence -- following -- a user -- a signature -- entering -- the contents -- using it -- a case -- this -- use -- strengthening -- a means -- having -- things -- the description -- ** -- carrying out -- the above -- (-- one --) -- a publication -- a system .

(5) The above-mentioned strengthening module is the system of the above-mentioned (1) publication characterized by having a means to guarantee that pursue the process generated from contents with a signature, and actuation of this process is in agreement with the requirements for a resource, and approval certification.

(6) The above-mentioned import device is the system of the above-mentioned (1) publication characterized by being the communication channel connected to the communication network.

(7) The above-mentioned import device is the system of the above-mentioned (1) publication characterized by being rotation storage.

(8) The above-mentioned import device is the system of the above-mentioned (1) publication characterized by being the memory card in which desorption is possible.

(9) ****** -- computer system -- memory -- having stored -- DS -- further -- having -- the above -- DS -- a signature -- entering -- contents -- a resource -- requirements -- a signature -- entering -- the contents -- having consumed -- being actual -- a resource -- and -- the above -- computer system -- a signature -- entering -- the contents -- having imposed -- either -- a resource -- a limit -- between -- correspondence -- being shown -- a table -- having -- things -- the description -- ** -- carrying out -- the above -- (-- one --) -- a publication -- a system .

(10) The above-mentioned table is the system of the above-mentioned (9) publication characterized by license conditions including further the constraint on the use imposed on contents with a signature.

(11) It is the memory which can read the computer which installed contents with a signature. The above-mentioned contents with a signature include the contents which can read the signature which can read a computer, and a computer. The signature which can read the above-mentioned computer in order to use the contents which can read the approval certification column and computer which are contained in the distribution chain of the contents which can read the above-mentioned computer, and which include code discernment of sending agency equipment and repeating installation at least It has two or more columns containing the requirements column for a resource which identifies a required computing resource.

(12) It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the license conditions [the above-mentioned part] which can read the computer relevant to the above-mentioned contents, The contents use system used in the computer system characterized by having the strengthening module which controls actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.

(13) The above-mentioned extractor is the system of the above-mentioned (1) publication characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

(14) The step which imports contents with a signature into computer system, The above-mentioned step which is a step which extracts the part of a signature from contents with a signature, and includes the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, The step which takes amendment actuation when the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are, The step which controls the operating system of the above-mentioned computer system to guarantee that use of contents with a signature does not exceed the requirements for a resource, and approval certification, How to guarantee the insurance of use of the contents with a signature in the above-mentioned computer system characterized by ****(ing).
(15) The approach of the above-mentioned (14) publication characterized by having further the step registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.
(16) The approach of the above-mentioned (14) publication characterized by having further the step which controls the above-mentioned operating system to guarantee that extract license conditions from a signature and contents with a signature are in agreement with license conditions.
(17) the above -- computer system -- memory -- inside -- a user -- approval -- certification -- and -- a signature -- entering -- the contents -- a function -- between -- correspondence -- being shown -- a table -- containing -- DS -- forming -- a step -- the above -- correspondence -- following -- a user -- a signature -- entering -- the contents -- using it -- a case -- this -- use -- strengthening -- a step -- further -- having -- things -- the description -- ** -- carrying out -- the above -- (-- 14 --) -- a publication -- an approach .
(18) The approach of the above-mentioned (14) publication characterized by having further the step which operates the above-mentioned process compulsorily so that it may be in agreement with the step and the requirements for a resource which pursue the process generated from contents with a signature, and approval certification.
(19) The contents with a signature are the approaches of the above-mentioned (14) publication characterized by having at least one of an application program and documents.
(20) How to control use of the contents in the above-mentioned computer system characterized by to have the step which imports into computer system contents including the license conditions which can read a computer, the step which extract the license conditions which can read a computer from the contents which imported, and the step which control actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.
(21) The approach of the above-mentioned (20) publication characterized by having further the step automatically registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is the epitome Fig. of the contents distribution device by the principle of this invention.

[Drawing 2] Drawing 2 shows the source and repeating installation in a contents distribution system.

[Drawing 3] Drawing 3 shows how repeating installation adds a signature to the contents under distribution according to the example of this invention with a manufacturer/author.

[Drawing 4] Drawing 4 shows the module contained when processing contents with a signature within a user's machine according to the example of this invention.

[Drawing 5] Drawing 5 shows the access information table which the strengthening module of drawing 4 uses.

[Drawing 6] Drawing 6 shows the relation between the capacity of the various entities of an insurance use system for the contents of drawing 4 .

[Drawing 7] Drawing 7 shows the relation between the privileges granted to a user who is different about the contents with a signature of the system of drawing 4 .

[Drawing 8] Drawing 8 shows the example of this invention in case contents with a signature are Java applets.

[Drawing 9] Drawing 9 shows action which the contents insurance use system of drawing 4 takes, when contents with a signature are received.

[Drawing 10] Drawing 10 shows how the strengthening module of drawing 4 strengthens security.

[Description of Notations]

1, 20, 30 User

2 Contents Insurance Use System

3 Operating System

4 11 Machine of a client

5 Contents Distribution Device

6, 23, 24, 25 Contents with a signature

7 List of Approval Certification

8 Requirements for Resource

10 Registration Information

12, 13, 14 Machine for junction

15, 16, 17 Machine of a manufacturer/author

21 Repeating Installation

22 Manufacturer/Author

32 Provider of Contents with Signature

33 Contents Import Device

34 Extractor

35 Analysis Module

36 Contents Interpretation Equipment

37 Strengthening Module

40 Access Information Table

42 Limit of Resource

43 Consumed Resource

44 Required Resource

50 Privilege of Operating System

51 User's Privilege

52 Privilege of Contents Insurance Use System

53 Privilege of Contents with Signature

54 Privilege of Generated Contents

60 User's Installed Privilege

61 User's 1 Privilege

62 User's 2 Privilege

63 User's 3 Privilege

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－91427

(43)公開日　平成10年(1998)４月10日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｚ
12/14	３１０	12/14	３１０Ｚ

審査請求　未請求　請求項の数21　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－151747

(22)出願日　平成９年(1997)６月10日

(31)優先権主張番号　０８／６６１６８７

(32)優先日　1996年６月11日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　ランガチャリ・アナンド
アメリカ合衆国07650、　ニュージャージー州パリセデス　パーク　ウィンドソール　ドライブ　544

(74)代理人　弁理士　坂口　博　（外１名）

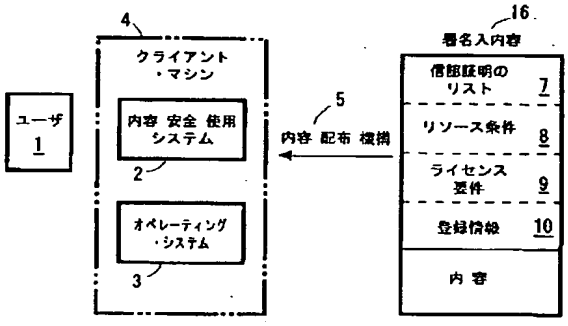
最終頁に続く

(54)【発明の名称】　署名入り内容の使用の安全を保証する方法及びシステム

(57)【要約】

【課題】　信頼性のないソースからネットワーク等を介して入手したソフトウェアを安全に実行するためのセキュリティー機構を提供する。

【解決手段】署名入り内容を配布する機構によってマシンにダウンロードするスキームを開示し、内容の性質には何らの制約が存在しないが、この内容上の署名は作成者の信認証明、リソース要件とライセンス情報を記述している。内容をダウンロードするとこれはクライアントのマシーン上で種々の方法によって使用することができる。これはクライアントのマシーンにインストールすることができ、その後ユーザはこれを実行することができる。この内容を使用するには、クライアントのマシーン上で演算リソースにアクセスする必要がある。演算システムの異なったサブセットに対するアクセスを許容及び規制するため、内容の署名に含まれる情報を使用するセキュリティー・マネージャーによってこのアクセスを補正する。



1

【特許請求の範囲】

【請求項１】内容移入機構と、

上記移入機構によって移入した署名入り内容を受け取るように接続され、上記署名入り内容から署名の部分を抽出する抽出装置であって、上記部分は上記内容と関連する信認証明と上記内容を使用するためのリソース要件とを含む上記抽出装置と、

上記抽出装置の供給した少なくとも信認証明を使用して署名入り内容の信頼性と完全性を確認し、信頼性と完全性の何れかに疑いのある場合には、補正動作をとる分析モジュールと、

署名入り内容の使用がリソース要件と信認証明に一致することを保証する強化モジュールと、

を有することを特徴とするコンピュータ・システムに於いて使用される内容安全使用システム。

【請求項２】上記抽出装置は署名から登録情報を抽出する手段を更に有し、ユーザに更に干渉することなく署名入り内容をプロバイダに登録する手段を更に有することを特徴とする請求項１記載のシステム。

【請求項３】上記抽出装置は署名からライセンス条件を抽出する手段を更に有し、上記強化モジュールはオペレーティング・システムと対話を行ってこの内容を使用することがライセンス条件に一致することを保証することを特徴とする請求項１記載のシステム。

【請求項４】上記コンピュータ・システムのメモリに格納したデータ構造を更に有し、上記データ構造はユーザ、信認証明及び署名入り内容の機能の間の対応を示すテーブルを有し、上記強化モジュールはデータ構造から対応テーブルを読み取るように接続され、上記対応に従ってユーザが署名入り内容を使用する場合にこの使用を強化する手段を有することを特徴とする請求項１記載のシステム。

【請求項５】上記強化モジュールは、署名入り内容から生成されたプロセスを追跡しこのプロセスの動作がリソース要件と信認証明に一致することを保証する手段を有することを特徴とする請求項１記載のシステム。

【請求項６】上記移入機構は、通信ネットワークに接続された通信チャンネルであることを特徴とする請求項１記載のシステム。

【請求項７】上記移入機構は、回転記憶装置であることを特徴とする請求項１記載のシステム。

【請求項８】上記移入機構は、脱着可能なメモリ・カードであることを特徴とする請求項１記載のシステム。

【請求項９】上記コンピュータ・システムのメモリに格納したデータ構造を更に有し、上記データ構造は署名入り内容、リソース要件、署名入り内容の消費した実際のリソース及び上記コンピュータ・システムが署名入り内容に課したいずれかのリソースの限度の間の対応を示すテーブルを有することを特徴とする請求項１記載のシステム。

2

【請求項１０】上記テーブルはライセンス条件が署名入り内容に課した使用上の制約を更に含むことを特徴とする請求項９記載のシステム。

【請求項１１】署名入り内容をインストールしたコンピュータの読み取り可能なメモリであって、上記署名入り内容はコンピュータの読み取り可能な署名とコンピュータの読み取り可能な内容を含み、上記コンピュータの読み取り可能な署名は上記コンピュータの読み取り可能な内容の配布チェーンに含まれている少なくとも発信元装置と中継装置の暗号識別を含む信認証明欄とコンピュータの読み取り可能な内容を使用するために必要なコンピューティング・リソースを識別するリソース要件欄を含む複数の欄を有している。

【請求項１２】内容移入機構と、

上記移入機構によって移入した署名入り内容を受け取るように接続され、上記署名入り内容から署名の部分を抽出する抽出装置であって、上記部分は上記内容と関連するコンピュータの読み取り可能なライセンス条件を含む上記抽出装置と、

署名入り内容の使用がライセンス条件に一致することを保証するように上記コンピュータ・システムの動作を制御する強化モジュールと、

を有することを特徴とするコンピュータ・システムに於いて使用される内容使用システム。

【請求項１３】上記抽出装置は署名から登録情報を抽出する手段を更に有し、ユーザに更に干渉することなく署名入り内容をプロバイダに登録する手段を更に有することを特徴とする請求項１記載のシステム。

【請求項１４】コンピュータ・システムに署名入り内容を移入するステップと、

署名入り内容から署名の部分を抽出するステップであって、上記部分は上記内容と関連する信認証明と上記内容を使用するためのリソース要件とを含む上記ステップと、

少なくとも信認証明を使用して署名入り内容の信頼性と完全性を確認し、信頼性と完全性の何れかに疑いのある場合には補正動作をとるステップと、

署名入り内容の使用がリソース要件と信認証明を超えないことを保証するように上記コンピュータ・システムのオペレーティング・システムを制御するステップと、

を有することを特徴とする上記コンピュータ・システムに於ける署名入り内容の使用の安全を保証する方法。

【請求項１５】署名から登録情報を抽出し、署名入り内容をユーザに更に干渉することなく通信チャンネルによってプロバイダに登録するステップを更に有することを特徴とする請求項１４記載の方法。

【請求項１６】署名からライセンス条件を抽出し、署名入り内容がライセンス条件と一致することを保証するように上記オペレーティング・システムを制御するステップを更に有することを特徴とする請求項１４記載の方

法。

【請求項１７】上記コンピュータ・システムのメモリ内にユーザ、信認の証明及び署名入り内容の機能の間の対応を示すテーブルを含むデータ構造を形成するステップと、上記対応に従ってユーザが署名入り内容を使用する場合にこの使用を強化するステップを更に有することを特徴とする請求項１４記載の方法。

【請求項１８】署名入り内容から生成されたプロセスを追跡するステップとリソース要件と信認証明に一致するように上記プロセスの動作を強制的に行うステップを更に有することを特徴とする請求項１４記載の方法。

【請求項１９】署名入り内容は、アプリケーション・プログラムとドキュメントの内の少なくとも１つを有することを特徴とする請求項１４記載の方法。

【請求項２０】コンピュータの読み取り可能なライセンス条件を含む内容をコンピュータ・システムに移入するステップと、

移入した内容からコンピュータの読み取り可能なライセンス条件を抽出するステップと、

署名入り内容の使用がライセンス条件と一致することを保証するように上記コンピュータ・システムの動作を制御するステップと、

を有することを特徴とする上記コンピュータ・システムに於ける内容の使用を制御する方法。

【請求項２１】署名から登録情報を抽出し、署名入り内容をユーザに更に干渉することなく通信チャンネルによってプロバイダに自動的に登録するステップを更に有することを特徴とする請求項２０記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、信頼性のないソースからネットワークまたはその他の手段によって入手したソフトウェアを安全に実行するためのコンピュータのセキュリティー機構に関する。

【０００２】

【従来の技術】ネットワーク化したコンピュータの有用性を増すため、これらのコンピュータがサーバから入手したプログラムを実行するのを可能にする方法が探求されている。ユーザからみた場合のこのようなシステムの主要な利点は、ユーザのコンピュータに格納しなければならないソフトウェアの量がこれによって少なくなることである。ソフトウェアのデベロッパーから見た場合、このシステムは多くの利点を有しているが、主要な利点は、アプリケーションのプロバイダがプログラムの配布に対してより統制を行うことができることである。World Wide Webのドキュメントに埋め込んだＪａｖａアプレット（即ち、プログラム）の使用は、このようなシステムの広く普及している例である。

【０００３】このようなアプローチに対する重要な関心事は、サーバから取得したソフトウェアが悪用を意図したものであり、ユーザのコンピュータを損傷しまたはデータを盗むかも知れないということである。従って、ダウンロードしたソフトウェアは、これらが必要とするシステムのリソースのみを与え、それ以上のものは与えない制御環境で実行しなければならない。現在用いられているＪａｖａアプレットのセキュリティー機構の主要な問題点は、これが十分な柔軟性を有していないことである。全てのＪａｖａアプレットは敵対的なものと考えられ、ユーザのマシンのオペレーティング・システム上の大部分のリソースにアクセスすることを許されていない。

【０００４】公開鍵暗号方式による認証のための標準的な技術には、種々のものが存在する。ＲＳＡは、幅広く使用されている公開鍵暗号アルゴリズムの一例である。これの実行例には、ＲＳＡｒｅｆとＰＧＰが含まれる。

【０００５】メッセージに対してディジタルの署名を作成する機構がまた存在している。これらの署名は人とメッセージの内容を結びつけるものである。これらは、メッセージの作成者がこのメッセージに対する責任を回避することができないように、メッセージに対してディジタルの署名を作成するためにまた使用することができる。ＲＳＡと組み合わせたＭＤ５アルゴリズムは、署名システムの一例である。

【０００６】多数のコンピュータ・オペレーティング・システムは、システムのリソースに対するアクセスを制御するための能力を使用している。１つの能力は、他のオブジェクトに対してあるアクションを実行するためにプロセスの保持している許可である。セキュリティーを強化するための能力を使用している著名なオペレーティング・システムには、ＡｍｏｅｂａとＭａｃｈがある。

【０００７】

【発明が解決しようとする課題】従って、本発明の目的は、信頼性のないソースからネットワークまたはその他の手段上で入手したソフトウェアを安全に実行するためのセキュリティー機構を提供することである。

【０００８】

【課題を解決するための手段】本発明の第１局面に従って、コンピュータ・システムに於いて使用する内容安全使用システムと方法を提供する。このシステムは、内容移入機構と、上記移入機構によって移入した署名入り内容を受け取るように接続され、上記署名入り内容から署名の部分を抽出する抽出装置であって、上記部分は上記内容と関連する信認証明を含む上記抽出装置と、上記内容を使用するリソース要件と、上記抽出装置の供給した少なくとも信認証明を使用して署名入り内容の信頼性と完全性を確認し、信頼性と完全性の何れかに疑いのある場合には、補正動作をとる分析モジュールと、署名入り内容の使用はリソース要件と信認証明に一致することを保証する強化モジュールとを有する。

【０００９】本発明の第２局面に従って、署名入り内容

5

をインストールしたコンピュータの読み取り可能なメモリを提供する。この署名入り内容は、コンピュータの読み取り可能な署名とコンピュータの読み取り可能な内容を含み、コンピュータの読み取り可能な署名はコンピュータの読み取り可能な内容の配布チェーンに含まれている少なくとも発信元装置と中継装置の暗号識別を含む信認証明欄とコンピュータの読み取り可能な内容を使用するために必要な演算リソースを識別するリソース要件欄を含む複数の欄を有している。

【００１０】本発明の第２局面に従って、コンピュータ・システム内でライセンス条件を強化する内容使用システムと方法が提供される。このシステムは、内容移入機構と、上記移入機構によって移入した署名入り内容を受け取るように接続され、上記署名入り内容から署名の部分を抽出する抽出装置であって、上記部分は上記内容と関連するコンピュータの読み取り可能なライセンス条件を含む上記抽出装置と、署名入り内容の使用がライセンス条件に一致することを保証するように上記コンピュータ・システムの動作を制御する強化モジュールとを有する。

【００１１】

【発明の実施の形態】本発明の実施例を、図を参照して詳細に説明する。図１によって、本発明を要約して説明する。ユーザ１は、クライアント・マシン４を使用し、かつ署名入り内容６をそのマシンに転送するための内容配布機構５を使用する。この配布機構の例には、フロッピー・ディスク、ＣＤ－ＲＯＭとインターネットが含まれる。実行可能な内容の例には、Ｊａｖａアプレット、ＯＬＥコンポーネンツとＳＯＭコンポーネンツが含まれる。この内容は、署名を有している。他の種類の内容は、テキスト、音声と映像を含むことができる。署名は４つの欄を有し、第１欄７は、ソフトウェアの信認証明のリストである。これは、図３で更に詳細に説明する。信認証明の例には、作者とメーカーの識別が含まれる。これらの証明は、その証明がリストに記載されている本人によって作成及び配布されたものであることを保証する。更に、これらの証明は、内容に署名した後この内容に対して変更が加えられていないことをチェックする手段を提供する。更に、作者はその作成した内容の責任を回避することができないことを保証する手段を、これらの証明は更に提供する。第２欄８は、内容がクライアントのマシン上で必要としているコンピューティング・リソース３を記述している。これらのリソースは、この内容がその目的をクライアント・マシン上で達成するために必要とされるものである。この目的の例には、署名入り内容のインストールと実行が含まれる。コンピューティング・リソースの例には、ディスクのスペース、ファイルのスペース、ファイルに対するアクセス、ＲＡＭ、ＣＰＵ、ネットワーク化の能力とユーザ・ディスプレイが含まれる。

6

【００１２】署名入り内容をユーザのマシンにダウンロードすると、ユーザはこの内容を種々の方法によって使用することができる。この内容を使用する例には、これをインストールすること、これを目視することとこれを実行することが含まれる。この内容は、クライアントのマシン上で慎重に制御した環境で使用する。署名入り内容をこのように使用するには、クライアントのマシン上で演算リソースにアクセスする必要がある。署名入り内容８を使用するために必要なリソースは、内容の署名の一部である。このようなリソースに対するアクセスは、内容安全使用システム２によって調停される。

【００１３】第３欄（これはオプションである）は、ライセンス情報９を提供するものである。ライセンス情報の例には、内容を使用することのできるマシンの数と期間のような使用条件が含まれる。第４欄（これはオプションである）は、登録情報１０である。この情報は、内容をプロバイダに自動的に登録するために使用する。図２は、内容配布機構の一例を示す。この内容はメーカまたは作者のマシン１５、１６、１７上で生起され、クライアントのマシン１１にダウンロードされる前に多数の中間のマシン１２、１３、１４を経由する。

【００１４】図３は、署名入り内容がメーカのマシン２２からユーザのマシン２０に配布されるのに従って、この署名入り内容に蓄積された証明を示す。メーカは、署名入り内容２５をある手段２７によって中継装置２１に転送する前に、この内容に信認証明を添付する。次に、この中継装置は、署名入り内容２４を配布チェーン内の次の中継装置に転送する前に、その信認証明をこの署名入り内容に添付する。このような方法で、署名入り内容が最終的にユーザに到達すると、これは全ての中継装置及びメーカ２３の信認証明のリストを含んでいる。

【００１５】図４は、内容安全使用システム３１内で内容のプロバイダ３１から署名入り内容をダウンロードするプロセスとこれに続くプロセスを示す。この内容安全使用システム３１は、ＩＢＭ　ＰＣパーソナル・コンピュータ、ＩＢＭ　ＲＳ／６０００ワークステーションまたはクライアントのシステムとして使用するのに適した他の何れかのワークステーションのような汎用コンピュータ・システム（図示せず）の一部として実施することができる。この署名入り内容は、内容移入システム３３によってダウンロードする。抽出装置３４は署名の欄を解析し、この情報を分析モジュール３５に引き渡す。この分析モジュールは内容の完全性を確認する。次にこの分析モジュールはセキュリティーの信認証明のリストを検討し、この内容をそのマシンで使用する場合のアクセスと信頼性のレベルを判定する。次に、この分析モジュールはこの内容のリソース要件を検討し、できればユーザの入力によって、これらの要件を満足することができるかどうかを判定する。次に、この情報を内容解釈装置３６と強化モジュール３７に引き渡す。

【００１６】内容移入機構３３は、例えば、ネットワーク・インタフェース（例えば、これによってユーザをインターネットに接続することができる）、ディスケット・サブシステム、ＣＤ　ＲＯＭサブシステムまたはカートリッジ記憶サブシステムとして実施することができる。抽出装置３４、分析モジュール３５、内容解釈装置３６と強化モジュール３７は、安全な内容を実行するワークステーションによって実行可能なプログラム・コードとして実施することができる。強化モジュールはワークステーションのオペレーティング・システム（ＯＳ／２、ＵＮＩＸまたはＷｉｎｄｏｗｓ　ＮＴのような）に接続するのが好ましい。内容解釈装置３６は、オペレーティング・システム内のモジュールとして実施することができるし、またはＪａｖａ解釈プログラムのように、オペレーティング・システムとは別個のものとすることができる。

【００１７】図９は、図４のシステムの動作に対応するフローチャートである。内容解釈装置は、内容を使用する機構である。内容解釈装置の例には、インターネットブラウザ及びＪａｖａ仮想マシンが含まれる。強化モジュールは分析モジュールの判定した信頼性のレベルを使用し、アクセス情報テーブル内に項目を作成する。このテーブルは、図５で説明する。

【００１８】署名入り内容を使用するには、一般的にオペレーティング・システムのリソースにアクセスする必要がある。図５は、そのマシン上で使用している署名入り内容の要求したまたはこの内容が消費したリソースを追跡するために強化モジュールが使用するテーブル４０を示す。強化モジュールは署名入り内容に関する信認証明４１を使用し、この署名入り内容がクライアントのマシン上で与えられるべきリソース４２の限度を判定する。この判定は、テーブルによる事前の構成と内容が得るべきアクセスを判定するためのユーザに対する明確な入力の要求を含む種々の方法によって行うことができる。「誰が何をどの程度アクセスするか」を反映する署名入り内容用の能力を強化モジュールが作成するのが効率的である。一般的に、署名入り内容が得るリソースはユーザがクライアントのマシン上でアクセスするリソースのサブセットである。セキュリティー・マネージャーは、内容によって消費されたリソース４３を追跡する。このことは、署名入り内容によるシステムのリソースに対する全てのアクセスがセキュリティー・マネージャーを通過することを保証することによって達成される。このテーブルは、署名入り内容の要求したリソース４３に対する項目をまた含んでいる。もし何れかの時点で、消費したリソース４３がリソースの限度４２または要求されたリソース４４を超えれば、セキュリティー・マネージャーは補正アクションをとることができる。補正アクションの例には、署名入り内容の使用の終了と、どのように進行するかについてのガイダンスのユーザに対する問い合わせが含まれる。

【００１９】図６は、種々の項目の能力の間の関係を示す。ユーザの特権５１は、オペレーティング・システム５０の特権のサブセットである。署名入り内容は、その特権５２がユーザの特権のサブセットである環境内で実行する。次に署名入り内容５３の特権はその実行環境のサブセットである。署名入り内容を使用することによって他の内容をクライアントのマシン上で使用することができる。例えば、Ｊａｖａアプレットを実行することによって他の実行可能な内容をクライアントのマシン上のプロセスにインストールすることができる。このように生成した内容５４の特権は署名入り内容と一致した特権のサブセットである。署名入り内容の署名にリソースの要件を包含することによって、セキュリティー・マネージャーにはこれらの制約を実行するための有効な機構が与えられることに留意してもらいたい。この生成した内容は、これの消費するリソースが署名入り内容に課されたリソースの限度である限り、実行することができる。この情報は、全て図５に示すセキュリティー・マネージャーのテーブル内で追跡することができる。

【００２０】署名入り内容をユーザのマシンにダウンロードすると、ユーザはこの内容を使用する能力を得る。この能力は、転送を開始したユーザと関連する。このユーザは他のユーザがこの署名入り内容をそのマシンで使用することを許す。図７は、６１、６２と６３のような他のユーザの特権とインストールを行っているユーザ２７の特権の間の関係を示す。例えば、署名入り内容がＬｏｔｕｓのドキュメントであれば、ユーザの特権はこのユーザがこのドキュメントを読み取れるか、このドキュメントに書き込みを行えるかまたはこのドキュメントを変更できるかに反映される。

【００２１】図８は、署名入り内容が署名を行ったＪａｖａアプレット８０である実施例を示す。このアプレット上の信認証明７９は、その作者、メーカー及び小売業者の信認証明である。このアプレットはサーバのマシン７７上に存在し、サーバのプロセス７８によって管理される。サーバのマシンとサーバのプロセスは単なる配布機構であり、これらは作者と何らの関係を有する必要がないことに留意する必要がある。内容配布機構は、インターネット７６である。

【００２２】ユーザ７１のために作用しクライアントのマシン７０上に存在するクライアントのエージェント７２が、サーバのプロセスとコンタクトすることによってアプレットをダウンロードする。このクライアントのエージェントは、ユーザの識別（その公開鍵または証明）のようなその信認証明またはクライアントのマシンの識別（ＩＰアドレス等）をサーバのプロセスに送付する。サーバ・プロセスはこの情報を使用し、ユーザの信頼できることを証明し、アプレットの使用を追跡する。これに応答して、サーバのプロセスは、署名入りアプレッ

ト、サーバのマシンの識別とこのサーバのプロセスの公開鍵（または証明）をクライアントに戻す。サーバはその応答をユーザの公開鍵によって暗号化し、アプレットがクライアントのマシンに安全に搬送されることを保証しなければならない。

【００２３】クライアントのエージェントは、内容の完全性及び関連する署名を確認する。これが行われると、クライアントのエージェントは信認の証明と署名入り内容のリソース要件を判定する。このエージェントはその秘匿復号鍵を使用してサーバの応答を復号し、応答内のセキュリティー情報即ち、作成者の識別（公開鍵または証明のような）、サーバのプロセスの識別（公開鍵または証明のような）とサーバのマシンの識別（ＩＰアドレスのような）を抽出する。この情報は、アプレットの名前、署名内に述べられているリソース要件、ユーザとクライアントのマシンの識別と共にセキュリティー強化装置７４に供給する。署名されたアプレットの信認証明は署名入り内容の名前、信認証明及び記述されたリソース要件によって構成されたトリプルによって構成される能力として格納され、セキュリティー・マネージャーに与えられる。

【００２４】セキュリティー強化装置は、Ｊａｖａが動作している時間の環境ではセキュリティー・マネージャーに類似している。それは変更することのできない信頼のあるシステム・サービスである。これは署名入り内容の信認証明を使用してアプレットをクライアントのマシン上で実行することのできる能力を演算する。実行上署名入り内容をセットすると、システムのリソースに対する全ての呼び出しは、セキュリティー・マネージャーを介して補正される。このセキュリティー・マネージャーはアプレットと関連する能力を使用し、アプレットの要求したリソースを許可するか否かを判定する（図１０）。このマネージャーをセキュリティーの政策の範囲をプログラムするために使用し、署名入りアプレットがシステムのリソースに対して有するアクセスを決定することができる。この政策の範囲は、アクセス無し、完全なアクセス、ユーザが予め構成したアクセスのような簡単な政策から始められ、アクセスはダイアログ・ボックスによってユーザをプロモートすることによって明確に許可される。

【００２５】アプレットをダウンロードするユーザは、他の誰がこれに対するアクセスを許可されているかを判定する。各ユーザに対して、特別の能力が作られる。内容がこれを行う場合、この内容は呼び出し者のアクセス権のサブセットによってこれを行う。いかなる時点でも、セキュリティー・マネージャーはアプレットのユーザに与えられた能力を取り消すことができる。

【００２６】本発明を好適な実施例によって説明したが、種々の変更と改善を当業者が行うことができる。従って、この好適な実施例は１例として提供されたものであり、限定を意図するものではないことを理解しなければならない。本発明の範囲は上記請求項によって明らかにされている。

【００２７】まとめとして、本発明の構成に関して以下の事項を開示する。

（１）内容移入機構と、上記移入機構によって移入した署名入り内容を受け取るように接続され、上記署名入り内容から署名の部分を抽出する抽出装置であって、上記部分は上記内容と関連する信認証明と上記内容を使用するためのリソース要件とを含む上記抽出装置と、上記抽出装置の供給した少なくとも信認証明を使用して署名入り内容の信頼性と完全性を確認し、信頼性と完全性の何れかに疑いのある場合には、補正動作をとる分析モジュールと、署名入り内容の使用がリソース要件と信認証明に一致することを保証する強化モジュールと、を有することを特徴とするコンピュータ・システムに於いて使用される内容安全使用システム。

（２）上記抽出装置は署名から登録情報を抽出する手段を更に有し、ユーザに更に干渉することなく署名入り内容をプロバイダに登録する手段を更に有することを特徴とする上記（１）記載のシステム。

（３）上記抽出装置は署名からライセンス条件を抽出する手段を更に有し、上記強化モジュールはオペレーティング・システムと対話を行ってこの内容を使用することがライセンス条件に一致することを保証することを特徴とする上記（１）記載のシステム。

（４）上記コンピュータ・システムのメモリに格納したデータ構造を更に有し、上記データ構造はユーザ、信認証明及び署名入り内容の機能の間の対応を示すテーブルを有し、上記強化モジュールはデータ構造から対応テーブルを読み取るように接続され、上記対応に従ってユーザが署名入り内容を使用する場合にこの使用を強化する手段を有することを特徴とする上記（１）記載のシステム。

（５）上記強化モジュールは、署名入り内容から生成されたプロセスを追跡しこのプロセスの動作がリソース要件と信認証明に一致することを保証する手段を有することを特徴とする上記（１）記載のシステム。

（６）上記移入機構は、通信ネットワークに接続された通信チャンネルであることを特徴とする上記（１）記載のシステム。

（７）上記移入機構は、回転記憶装置であることを特徴とする上記（１）記載のシステム。

（８）上記移入機構は、脱着可能なメモリ・カードであることを特徴とする上記（１）記載のシステム。

（９）上記演コンピュータ・システムのメモリに格納したデータ構造を更に有し、上記データ構造は署名入り内容、リソース要件、署名入り内容の消費した実際のリソース及び上記コンピュータ・システムが署名入り内容に課したいずれかのリソースの限度の間の対応を示すテー

ブルを有することを特徴とする上記（１）記載のシステム。

（１０）上記テーブルはライセンス条件が署名入り内容に課した使用上の制約を更に含むことを特徴とする上記（９）記載のシステム。

（１１）署名入り内容をインストールしたコンピュータの読み取り可能なメモリであって、上記署名入り内容はコンピュータの読み取り可能な署名とコンピュータの読み取り可能な内容を含み、上記コンピュータの読み取り可能な署名は上記コンピュータの読み取り可能な内容の配布チェーンに含まれている少なくとも発信元装置と中継装置の暗号識別を含む信認証明欄とコンピュータの読み取り可能な内容を使用するために必要なコンピューティング・リソースを識別するリソース要件欄を含む複数の欄を有している。

（１２）内容移入機構と、上記移入機構によって移入した署名入り内容を受け取るように接続され、上記署名入り内容から署名の部分を抽出する抽出装置であって、上記部分は上記内容と関連するコンピュータの読み取り可能なライセンス条件を含む上記抽出装置と、署名入り内容の使用がライセンス条件に一致することを保証するように上記コンピュータ・システムの動作を制御する強化モジュールと、を有することを特徴とするコンピュータ・システムに於いて使用される内容使用システム。

（１３）上記抽出装置は署名から登録情報を抽出する手段を更に有し、ユーザに更に干渉することなく署名入り内容をプロバイダに登録する手段を更に有することを特徴とする上記（１）記載のシステム。

（１４）コンピュータ・システムに署名入り内容を移入するステップと、署名入り内容から署名の部分を抽出するステップであって、上記部分は上記内容と関連する信認証明と上記内容を使用するためのリソース要件とを含む上記ステップと、少なくとも信認証明を使用して署名入り内容の信頼性と完全性を確認し、信頼性と完全性の何れかに疑いのある場合には補正動作をとるステップと、署名入り内容の使用がリソース要件と信認証明を超えないことを保証するように上記コンピュータ・システムのオペレーティング・システムを制御するステップと、を有することを特徴とする上記コンピュータ・システムに於ける署名入り内容の使用の安全を保証する方法。

（１５）署名から登録情報を抽出し、署名入り内容をユーザに更に干渉することなく通信チャンネルによってプロバイダに登録するステップを更に有することを特徴とする上記（１４）記載の方法。

（１６）署名からライセンス条件を抽出し、署名入り内容がライセンス条件と一致することを保証するように上記オペレーティング・システムを制御するステップを更に有することを特徴とする上記（１４）記載の方法。

（１７）上記コンピュータ・システムのメモリ内にユーザ、信認の証明及び署名入り内容の機能の間の対応を示すテーブルを含むデータ構造を形成するステップと、上記対応に従ってユーザが署名入り内容を使用する場合にこの使用を強化するステップを更に有することを特徴とする上記（１４）記載の方法。

（１８）署名入り内容から生成されたプロセスを追跡するステップとリソース要件と信認証明に一致するように上記プロセスの動作を強制的に行うステップを更に有することを特徴とする上記（１４）記載の方法。

（１９）署名入り内容は、アプリケーション・プログラムとドキュメントの内の少なくとも１つを有することを特徴とする上記（１４）記載の方法。

（２０）コンピュータの読み取り可能なライセンス条件を含む内容をコンピュータ・システムに移入するステップと、移入した内容からコンピュータの読み取り可能なライセンス条件を抽出するステップと、署名入り内容の使用がライセンス条件と一致することを保証するように上記コンピュータ・システムの動作を制御するステップと、を有することを特徴とする上記コンピュータ・システムに於ける内容の使用を制御する方法。

（２１）署名から登録情報を抽出し、署名入り内容をユーザに更に干渉することなく通信チャンネルによってプロバイダに自動的に登録するステップを更に有することを特徴とする上記（２０）記載の方法。

【図面の簡単な説明】

【図１】図１は、本発明の原理による内容配布機構の要約図である。

【図２】図２は、内容配布システムに於けるソースと中継装置を示す。

【図３】図３は、メーカ／作者と中継装置が本発明の実施例に従ってどのようにして配布中の内容に署名を付加するかを示す。

【図４】図４は、本発明の実施例に従ってユーザのマシン内で署名入り内容を処理する場合に含まれているモジュールを示す。

【図５】図５は、図４の強化モジュールの使用するアクセス情報テーブルを示す。

【図６】図６は、図４の内容を安全使用システムの種々のエンティティの能力の間の関係を示す。

【図７】図７は、図４のシステムの署名入り内容について異なったユーザに与えられる特権の間の関係を示す。

【図８】図８は、署名入り内容がＪａｖａアプレットである場合の本発明の実施例を示す。

【図９】図９は、署名入り内容を受け取った場合に、図４の内容安全使用システムの取るアクションを示す。

【図１０】図１０は、図４の強化モジュールがセキュリティーを強化する方法を示す。

【符号の説明】

１、２０、３０　ユーザ

２　　内容安全使用システム

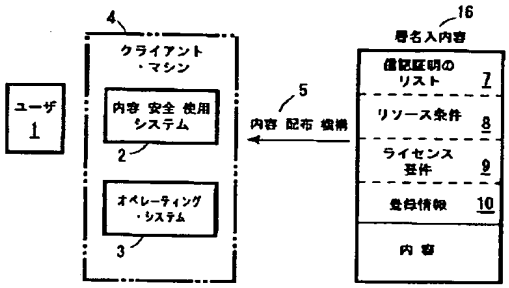
13

３　オペレーティング・システム
４、１１　クライアントのマシン
５　内容配布機構
６、２３、２４、２５　署名入り内容
７　信認証明のリスト
８　リソース要件
１０　登録情報
１２、１３、１４　中継用マシン
１５、１６、１７　メーカー／作者のマシン
２１　中継装置
２２　メーカー／作者
３２　署名入り内容のプロバイダ
３３　内容移入機構
３４　抽出装置
３５　分析モジュール

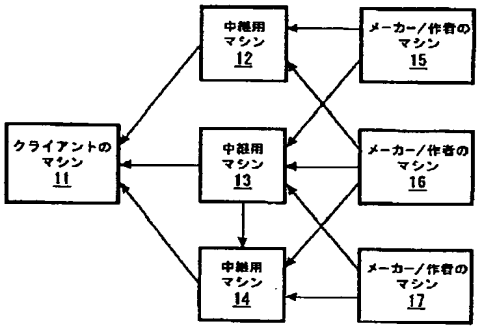
14

＊３６　内容解釈装置
３７　強化モジュール
４０　アクセス情報テーブル
４２　リソースの限度
４３　消費したリソース
４４　必要なリソース
５０　オペレーティング・システムの特権
５１　ユーザの特権
５２　内容安全使用システムの特権
５３　署名入り内容の特権
５４　生成した内容の特権
６０　インストールしたユーザの特権
６１　ユーザ１の特権
６２　ユーザ２の特権
＊　６３　ユーザ３の特権

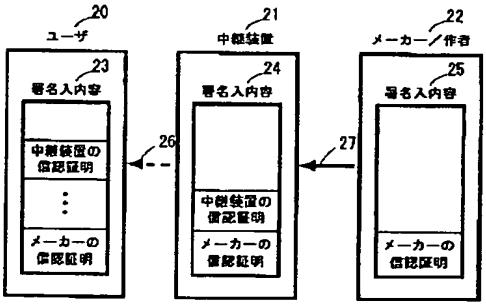
【図１】



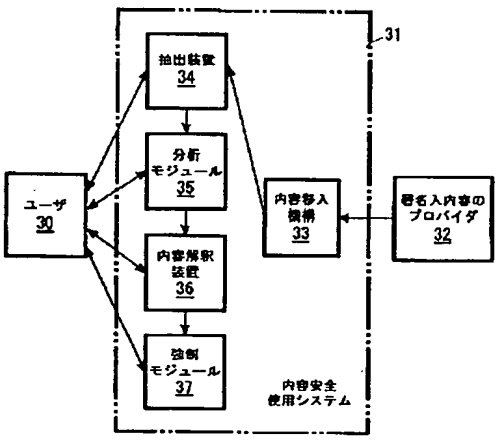
【図２】



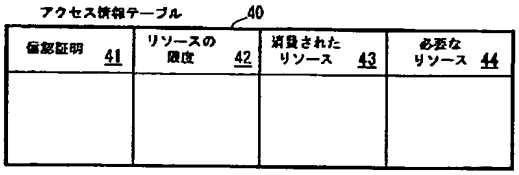
【図３】



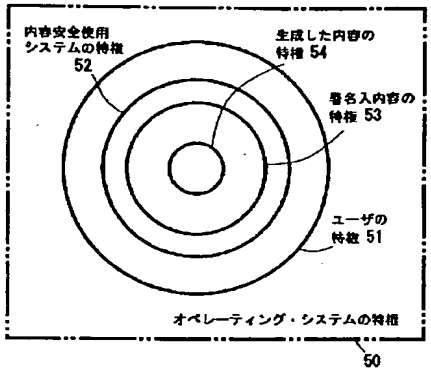
【図４】



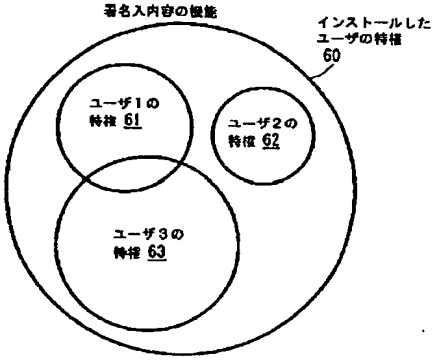
【図５】



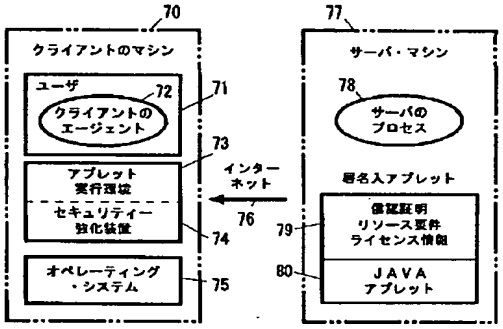
【図６】



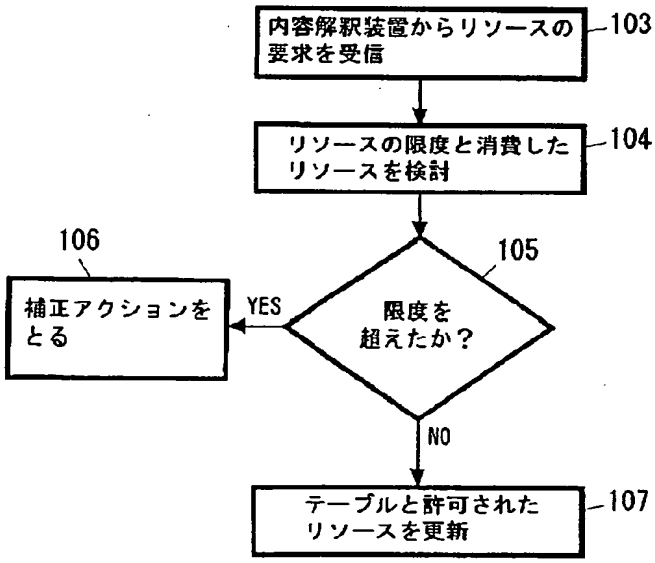
【図７】



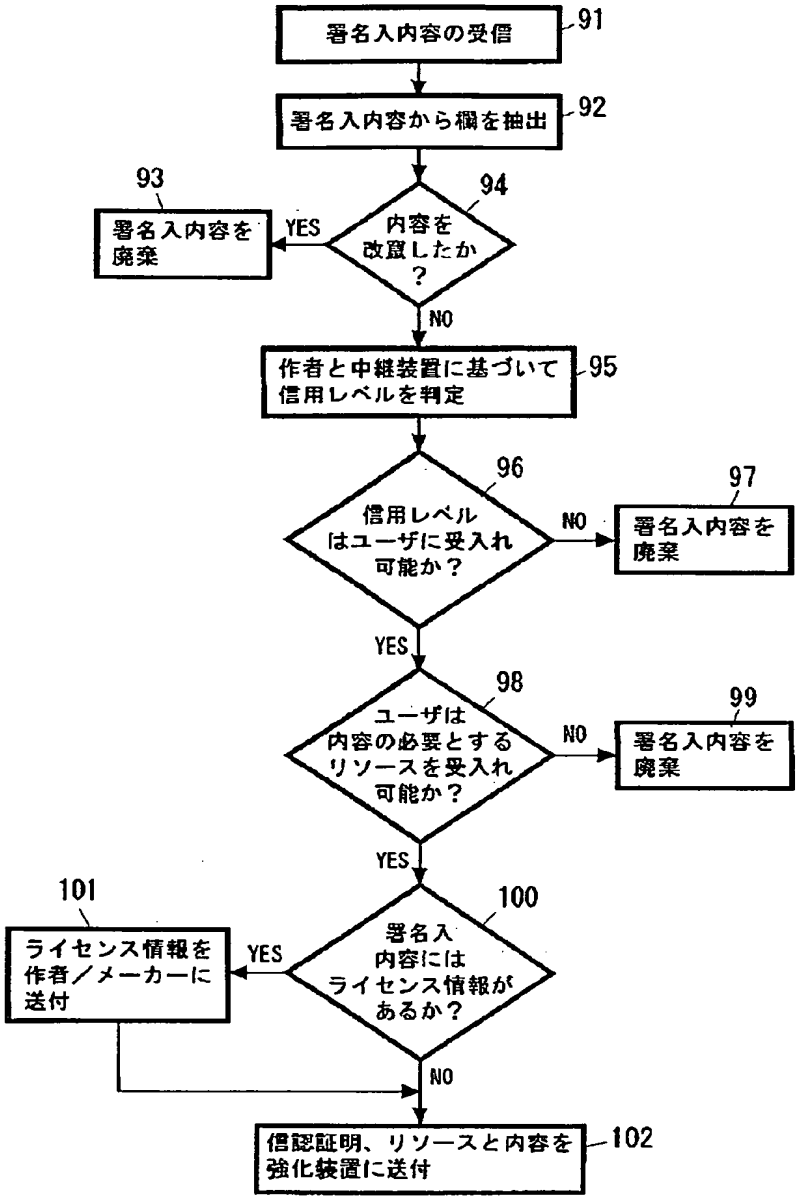
【図８】



【図１０】



【図９】



フロントページの続き

(72)発明者　ナイーム・イスラム
アメリカ合衆国10598、　ニューヨーク州　ヨークタウン　ハイツ　シェニック　ビュー　５　アパートメント　Ａ

(72)発明者　ジョスユラ・ラマチャンドラ・ラオ
アメリカ合衆国10510、　ニューヨーク州　ブライアークリフ　マノール　オーチャード　ロード　151　＃３Ａ